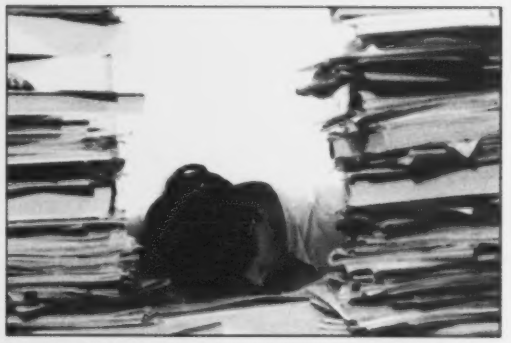
January 2010

FOIP FOLIO

WORKLOAD AT THE OIPC

For the first nine months of this fiscal year, we have opened 220 case files (access reviews and privacy investigations). This is an **increase of 113%** over the 103 case files opened for the same period one year ago. In the result, we had as at January 1, 2010, a caseload of **367 active files**. This translates into a caseload of about 130 files for each of our three Portfolio Officers. In February, we will be discussing with the Board of Internal Economy strategies to cope with this dramatic increase in investigative work.



B.C. ACCESS AND PRIVACY COMMISSIONER MOVING ON

David Loukidelis, British Columbia Information and Privacy Commissioner, has resigned his position to assume a new role as Deputy Attorney General in the Ministry of the Attorney General. David has been a wonderful resource to our OIPC and is one of the most knowledgeable individuals in the country on access to information and the protection of privacy.

(Continued on page 2)

INSIDE THIS ISSUE

Workload at the OIPC.....1

B.C. Access & Privacy Commissioner Moving On.....1

January 28—Privacy Day.....2

Report LA-2009-01/H-2009-001 (Regina Qu'Appelle Regional Health Authority).....2

Outpacing Change.....3

What to do as a Trustee when a Patient Disagrees with their Personal Information as Recorded.....3

New Changes to Federal Privacy Laws?.....3

Encrypt your Mobile Devices: Do It Now!.....4

Recommended Reading.....4

SK Gaming Corp. (SGC) Makes Positive Changes.....5

FAQs for Administrative Tribunals.....5

USA Federal Trade Commission—A new , more aggressive Focus on Privacy Protection for Consumers.....6

Frivolous Requests, Abusive Requesters— A Nova Scotia Perspective.....6

AB OIPC Revises Inquiry Procedures.....6

B.C. Special Legislative Committee Undertaking Access and Privacy Review.....7

Another Perspective on Electronic Health Records.....7

Ontario Rights Case Permits Use and Disclosure of Individual's PHI.....7

N.B. Court Orders Production of Facebook Use.....8

Mark Your Calendar.....8

(Continued from page 1)

From his steady, pragmatic oversight of B.C.'s fledgling *Personal Information Protection Act* to his thorough approach to issues raised by the B.C. public / public bodies and his review of the implications of the *USA Patriot Act,* he has made a large and enduring contribution to information rights in Canada. All of us at the OIPC wish him well in his new challenge!

JANUARY 28—PRIVACY DAY

January 28th is celebrated as **'Privacy Day'** in most of the European Union nations, the U.S. and much of Canada. This date was originally chosen since it is the anniversary of the approval of the European Convention 108. This is an excellent excuse for organizations to assess how well their public body or health trustee is doing in managing its statutory responsibilities to protect the privacy of Saskatchewan residents. For your assistance, our office has produced a number of tools available on our website including:

Privacy Breach Guidelines

Video Surveillance Guidelines

Best Practices – Mobile Device Security

Privacy Considerations – Faxing Personal Information and Personal Health Information

Frequently Asked Questions – Administrative Tribunals and Internet Publication of Decisions

Archived copies of 64 past issues of the *Saskatchewan FOIP FOLIO*

Breach of Privacy Reports of OIPC including Investigation Reports F-2009-001, F-2007-001, F-2005-001, LA-2005-003, H-2007-001, H-2005-002, H-2004-001

You can find information about Privacy Day and related events at the websites of Canada's Information and Privacy Commissioners. You can find links through our website at www.oipc.sk.ca under the 'links; tab.

REPORT LA-2009-001/H-2009-001 (REGINA QU'APPELLE REGIONAL HEALTH AUTHORITY)

Our office issued Report LA-2009-002 / H-2009-001 in December, 2009. This related to an access request from the estate of a former patient of Regina Qu'Appelle Regional Health Authority (RQRHA) for the personal health information of that patient. A number of exemptions were raised by the RQRHA and then addressed in the Report. A key issue was whether the applicant was making a request for records related to "administration of the estate." The Commissioner held that given the relevant laws in Saskatchewan, this test was met. There is also extensive discussion of the duty to assist that is required of all health trustees in Saskatchewan. The Report is available at our website, www.oipc.sk.ca under the 'Reports' tab.

OUTPACING CHANGE

Ernst & Young has published its 12th annual global information security survey. Some key findings are that:

Few companies are encrypting their laptops. Only 41% of respondents are encrypting them today, with 17% planning to do so in the next year.

41% of respondents noted an increase in external attacks and 25% of respondents witnessed an increase in internal reports.

75% of respondents revealed that they are concerned with the possible reprisal from employees recently separated from their organization.

In 2009, the primary challenge to effectively delivering information security was the lack of appropriate resources.

You can read the full report at: www.ey.com.

WHAT TO DO AS A TRUSTEE WHEN A PATIENT DISAGREES WITH THEIR PERSONAL INFORMATION AS RECORDED

In all three of the laws that our office oversees (FOIP s. 32, LA FOIP s. 31 and HIPA s. 40), there is provision for an individual to request that a government institution, local authority or health trustee make a correction of their personal information or personal health information (phi) in the record that concerns them. If the public body or trustee refuses to do so, they must still make a notation in the record of the requested amendment. Our office has not yet had occasion to discuss what exactly a notation should look like but we note a recent Alberta Order from the Alberta Information and Privacy Commissioner (IPC) that is relevant. Keeping in mind that Alberta's *Health Information Act* sets out a more fulsome duty than its Saskatchewan counterpart to receive and retain a 'statement of disagreement' of up to 500 words, the discussion is nonetheless helpful. It canvasses a number of issues about the appropriate content and what exactly is required by statute. It also canvasses a number of Ontario IPC Orders and previous Alberta OIPC Orders and a relevant court decision. Order H2009-001 is available at the website, www.oipc.ab.ca.

NEW CHANGES TO FEDERAL PRIVACY LAWS?

Tony Clement, Canada's Industry Minister, announced on January 4, 2010, that one of his priorities in the New Year will be promoting the development of Canada's 'digital economy'. He plans to do this by introducing legislation that modernizes Canada's privacy laws. For more information, see http://www.canada.com/story_print.html?id=2403662&sponsor.

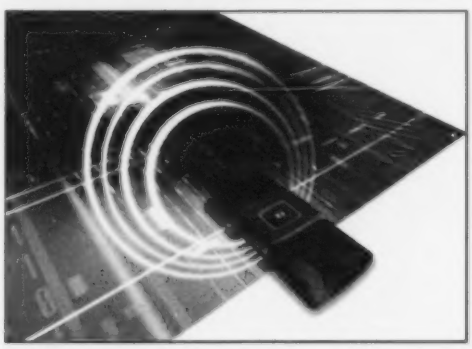
ENCRYPT YOUR MOBILE DEVICES: DO IT NOW

In December 2009, the Ontario IPC was notified that a public health nurse working for the Durham Health Department had lost a USB memory stick containing the phi of 83,524 individuals who had attended H1N1 immunization clinics. The memory stick was lost as the nurse walked from the clinic to her car in the parking lot. Commissioner **Ann Cavoukian** noted that three years ago following the loss of a laptop computer containing phi she had sent a clear message to custodians against storing unencrypted personal health information on mobile devices. She observed that "The fact that three years later, health care providers would be unaware of this requirement is both disappointing and unacceptable." The Commissioner made a number of recommendations to ensure that all public health unit staff is aware of the need for proper safeguards for phi stored on mobile devices. Key recommendations were that when phi must be stored on mobile devices, the following measures are necessary:

- Only the *minimal amount* of information necessary should be stored, and for the *minimal amount of time* necessary to complete the work;
- Whenever possible, phi should be *de-identified or coded*, in a manner such that the identities of the individuals whose phi is stored on the device could not be readily ascertained if the information were accessed by unauthorized persons;
- If the information is coded, the code that is needed to unlock the identities of individuals should be stored separately on a secure computing device, such as a central server in a health care facility;
- The use of *strong password protection*; and, most important,
- The use of *strong encryption*.

The full PHIPA Order HO-007 is available at www.ipc.on.ca.

The Saskatchewan OIPC takes a similar view and supports those recommendations that mirror the position taken by other Canadian privacy oversight offices. We discussed the need to encrypt a memory stick in our September 2008 FOIP FOLIO, page 5.



RECOMMENDED READING: *BUYING YOU—THE GOVERNMENT'S USE OF FOURTH-PARTIES TO LAUNDER DATA ABOUT "THE PEOPLE"*

This is the title of a fascinating article written by **Joshua L. Simmons** for the Columbia 'Business Law Review.' This issue has become very topical given the significant amount of recent

Canadian case law that deals with Internet Service Providers transferring subscriber data to police and investigative agencies often without warrant. You can access this at 2009 Columb. Bus. L. Rev. 950.

POSITIVE CHANGES MADE BY SASKATCHEWAN GAMING CORPORATION (SGC)

The casinos in Regina and Moose Jaw will now allow individuals to purchase tickets to events in the show lounge without a requirement that the purchaser for cash must also provide personal information including name, address, phone number and email address. There is new signage in the area of the ticket booth, a new brochure and all of this has been complemented by staff training on requirements of FOIP. Patrons who wish to be notified in the event of cancellation of a show or who wish to be able to easily obtain a refund can still provide the contact information if they so choose. The SGC is a 'government institution' that operates those two casinos. The changes followed complaints to the OIPC in late 2008 and a subsequent OIPC investigation. Congratulations to SGC Privacy Officer **Lynn Armstrong** and her staff for all of these new compliance measures.

FAQs FOR ADMINISTRATIVE TRIBUNALS

The distinguished administrative law expert **David Phillip Jones, Q.C.** recently observed in a presentation to a national audience of lawyers in Ottawa that *"Privacy laws continue to add a whole new element to administrative law."* Coincidentally but consistent with Mr. Jones comment, a set of Frequently Asked Questions (FAQs) have been developed by Canada's privacy commissioners to assist administrative tribunals who are publishing personal information on the Internet or are contemplating such publication. These FAQs identify questions that administrative tribunals need to ask before Internet publication. Transparency in how public agencies do their business is certainly important. A number of these administrative tribunals are also 'government institutions' for purposes of FOIP and need to ensure that they are considering the privacy requirements in Part IV of FOIP and particularly the limitations on disclosure of personal information. In some cases, these administrative tribunals are also 'trustees' for purposes of HIPA and have additional obligations to consider.

The FAQs also offer suggestions on things that can be done by those tribunals that are mandated to publish on the Internet to minimize the risk of harm to individuals and thus to comply with the applicable privacy laws. You can access these FAQs at our website: www.oipc.sk.ca under the 'Resources' tab. At the website you can also find a resource list compiled by our office. You may wish to review our Investigation Report F-2005-001 (Automobile Injury Appeal Commission) which considered many of these questions. This is available at www.oipc.sk.ca under the 'Reports' tab. There are also published papers from the IPCs of British Columbia and Saskatchewan at *Privacy and Openness in Administrative Tribunal Decisions*, CJALP, Vol. 22, No. 1 February 2009, p. 75 and *Administrative Tribunals, Privacy and the Net*, Canadian Privacy Law Review, Vol. 6, No. 8, July 2009, p. 65 respectively.

USA FEDERAL TRADE COMMISSION—A NEW, MORE AGGRESSIVE FOCUS ON PRIVACY PROTECTION FOR CONSUMERS

For U.S. based companies doing business in Saskatchewan our federal private sector privacy law (*Personal information Protection and Electronic Documents Act* or PIPEDA) has always been something of a surprise and a mystery. This is largely because although there is in the U.S. a web of state sector–specific privacy laws, there is no comprehensive, national privacy law which applies to the broad private sector of the economy. That may be changing. The traditional reliance on self regulation has not proven particularly effective. The Federal Trade Commission (FTC) has a new chairman who has signalled a much greater focus on privacy issues. There have been extensive consultations and roundtable discussions by the FTC. There is also an expectation of increased legislative activity in this area by Congress. Those American companies that have had to develop PIPEDA compliance practices for their commercial activity in Canada may soon be in the position of industry leaders in their own nation. For more information on FTC activities, go to http://www.ftc.gov.

FRIVOLOUS REQUESTS, ABUSIVE REQUESTERS—A NOVA SCOTA PERSPECTIVE

The Nova Scotia Review Officer, **Dulcie McCallum**, has recently issued a Report involving the interaction between an applicant for access to records and the Department of Community Services. In her Report FI-08-35/FI-08-54, the Review Officer discusses the demeaning and condescending language of the applicant in his dealings with the public body. She notes that the Nova Scotia *Freedom of Information and Protection of Privacy Act*, much like its Saskatchewan counterpart, does not allow a Department to refuse a request that is trivial, frivolous, vexatious or not made in good faith. She recommends that the government give *"strong consideration to proposing such an amendment in any future legislative review."* We have made a similar recommendation to our Legislative Assembly in past Annual Reports. The Nova Scotia Report is available at www.foipop.ns.ca.

ALBERTA OIPC REVISES INQUIRY PROCEDURES

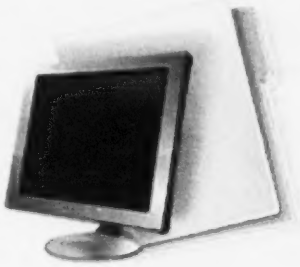
In late 2009, Alberta Commissioner **Frank Work** announced a set of changes to streamline the inquiry process in that jurisdiction and to make it more efficient. You can view these changes in the Alberta OIPC process at www.oipc.ab.ca under the `Resources` tab.

BRITISH COLUMBIA SPECIAL LEGISLATIVE COMMITTEE UNDERTAKING ACCESS AND PRIVACY REVIEW

Every six years the *Freedom of Information and Protection of Privacy Act* (BC FOIP) in British Columbia requires that the government strike a Special Committee of the Legislature to review their BC FOIP Act. That Committee was created on October 5, 2009 and members of the public have until February 28, 2010 to make a submission. There have been at least two earlier such reviews since the B.C. law went into force in 1994. Alberta has done a similar number of public reviews of their FOIP Act. Our office has recommended that this province undertake a similar review in past Annual Reports. Saskatchewan is one of the few jurisdictions that has not undertaken any formal review of FOIP since it went into force in 1992.

ANOTHER PERSPECTIVE ON ELECTRONIC HEALTH RECORDS

An interesting article in the 'National Law Journal' on December 14, 2009 – *Electronic health records pose several challenges* certainly gives pause for thought. Since the rollout of different components of the electronic health record (EHR), questions have arisen as to how this will impact litigation that involves medical records. After all, EHRs have been described as *"abstractions composed of thousands of data elements in relational databases that may include data hosted by business associates of the organization or other providers and payers."* Which screen shots will be needed to be produced as the official medical record? Will a party to medical litigation be required to produce all data in every redundant viewable format? The authors, **Jason E. Christ** and **Robert J. Hudock** state:



"Given the compelling public interest furthered by EHRs, it's time to consider alternatives to the use of overly broad production and preservation requests as settlement leverage. In order to facilitate the use and success of EHRs, the legal community should depart from viewing electronic health records as static documents that can be printed, stamped and produced, and move toward producing or otherwise making available the EHR in a responsible manner that takes into account efficiency, expense and the goals of the proceeding."

ONTARIO RIGHTS CASE PERMITS USE AND DISCLOSURE OF INDIVIDUAL'S PERSONAL HEALTH INFORMATION (PHI)

The Human Rights Tribunal of Ontario, in a December 2009 decision, permitted the use and disclosure of phi of an individual by a physician who was the subject of a discrimination complaint. The Tribunal considered the Ontario *Personal Health Information Protection Act* and determined that the consent of the individual was not necessary for the use or disclosure of the individual's phi for the purpose of the proceeding under the Human Rights Code. You can read the decision at 2009 HRTO 1834 (CanLII). Although we are not aware that this issue has arisen in Saskatchewan, the relevant sections of HIPA would presumably be section 27(4)(i), (l) and (m).

NEW BRUNSWICK COURT ORDERS PRODUCTION OF FACEBOOK USE

In early December 2009, the Court of Queen's Bench of New Brunswick ordered a plaintiff in a motor vehicle accident case to produce a record of her activities on Facebook. The decision is notable for the thorough treatment of the privacy issue by the presiding judge. An interesting observation by the judge was that, *"It must not be forgotten that this legal action was commenced by the Plaintiff and in launching it she has implicitly accepted certain intrusions into what otherwise might be private information the disclosure of which would ordinarily be left to her own judgment. Of course these intrusions are subject to the implied undertaking of confidentiality except with respect to the ongoing proceeding."* The full report is available at 2009 NBQB 317 (CanLII).

MARK YOUR CALENDAR!

Canadian Bar Association Privacy and Access Law Section meetings in Regina and Saskatoon. To register for any of the following section meetings call CBA at (306) 244-3898

Saskatoon

- **February 8, 2010:** *Privacy and Access Law North*, Saskatoon Club, Saskatoon at 12:00 noon. Topic: Workplace Privacy Issues. Speakers: Kaylea Dunn and David Stack, McKercher LLP.

Regina

- **February 8, 2010:** Privacy and Access Law South (CBA section meeting), Hotel Saskatchewan, Regina at 12;00 noon. Topic: Solicitor-Client Privilege and Access to Information Requests. Speaker: TBA. To register call Lorraine at (306) 244.3898

February 9—10, 2010: *11th Annual Privacy and Security Conference*, Victoria, British Columbia. For more information, visit www.rebootconference.com/privacy2010/

April 19—21, 2010: *IAPP Global Privacy Summit*, Washington, D.C. For more information, visit www.privacysummit.org/

June 9—11, 2010: *2010 Access and Privacy Conference*, Marriott Hotel, River Cree Resort, Edmonton, Alberta. For more information, visit www3.extension.ualberta.ca/accessandprivacy/

OFFICE OF THE SASKATCHEWAN INFORMATION AND PRIVACY COMMISSIONER

503 – 1801 Hamilton Street
Regina, Saskatchewan
S4P 4B4

Telephone: (306) 787-8350 / Toll Free: 1-877-748-2298
Fax: (306) 798-1603
E-mail: webmaster@oipc.sk.ca

Website: www.oipc.sk.ca

If you wish to subscribe to the Saskatchewan FOIP FOLIO, please send your e-mail address to webmaster@oipc.sk.ca.